Kerberos et interopérabilité

Guillaume Rousse

INRIA Saclay - Ile de France

Mardi 24 mai 2010

Plan

Plan

Présentation

Description

Kerberos est un protocole d'authentification, sécurisé, de type SSO

Caractéristiques

- authentification
- sécurisé
- SSO

Présentation

Description

Kerberos est un protocole d'authentification, sécurisé, de type SSO

Caractéristiques

- authentification
- sécurisé
- SSO

Histoire

projet Athena

- projet commun MIT, DEC et IBM
- X Windows

Kerberos 4

- fin des années 1980
- utilisation au sein d'AFS

Kerberos 5

- 1993
- première spécification

Histoire

projet Athena

- projet commun MIT, DEC et IBM
- X Windows

Kerberos 4

- fin des années 1980
- utilisation au sein d'AFS

Kerberos 5

- 1993
- première spécification

Histoire

projet Athena

- projet commun MIT, DEC et IBM
- X Windows

Kerberos 4

- fin des années 1980
- utilisation au sein d'AFS

Kerberos 5

- 1993
- première spécification

Standardisation

RFCs

- 1993 : RFC 1510 (kerberos)
- 2005 : RFC 3961 (encryption)
- 2005 : RFC 3962 (AES)
- 2005 : RFC 4120 (kerberos)
- 2005 : RFC 4121 (GSSAPI)

Foire aux acronymes

- GSSAPI
- SPNEGO

Standardisation

RFCs

- 1993 : RFC 1510 (kerberos)
- 2005 : RFC 3961 (encryption)
- 2005 : RFC 3962 (AES)
- 2005 : RFC 4120 (kerberos)
- 2005 : RFC 4121 (GSSAPI)

Foire aux acronymes

- GSSAPI
- SPNEGO

Concepts

Royaume

- unité d'organisation de Kerberos
- en général, MON.ROYAUME = mon.domaine

Principal

- entité correspondant à un utilisateur ou une machine
  - utilisateur@MON.ROYAUME
  - utilisateur/instance@MON.ROYAUME

Key Distribution Center

- élément central d'un royaume
- base de tous les principaux du royaume
- serveur d'authentification et de distribution des clés

Concepts

Royaume

- unité d'organisation de Kerberos
- en général, MON.ROYAUME = mon.domaine

Principal

- entité correspondant à un utilisateur ou une machine
  - utilisateur@MON.ROYAUME
  - utilisateur/instance@MON.ROYAUME

Key Distribution Center

- élément central d'un royaume
- base de tous les principaux du royaume
- serveur d'authentification et de distribution des clés

Concepts

Royaume

- unité d'organisation de Kerberos
- en général, MON.ROYAUME = mon.domaine

Principal

- entité correspondant à un utilisateur ou une machine
  - utilisateur@MON.ROYAUME
  - utilisateur/instance@MON.ROYAUME

Key Distribution Center

- élément central d'un royaume
- base de tous les principaux du royaume
- serveur d'authentification et de distribution des clés

Plan

Principe

Acteurs

- client
- service
- KDC

Actes

- le client s'authentifie auprès du KDC
- le client demande un ticket de service au KDC
- le client accède au service

Principe

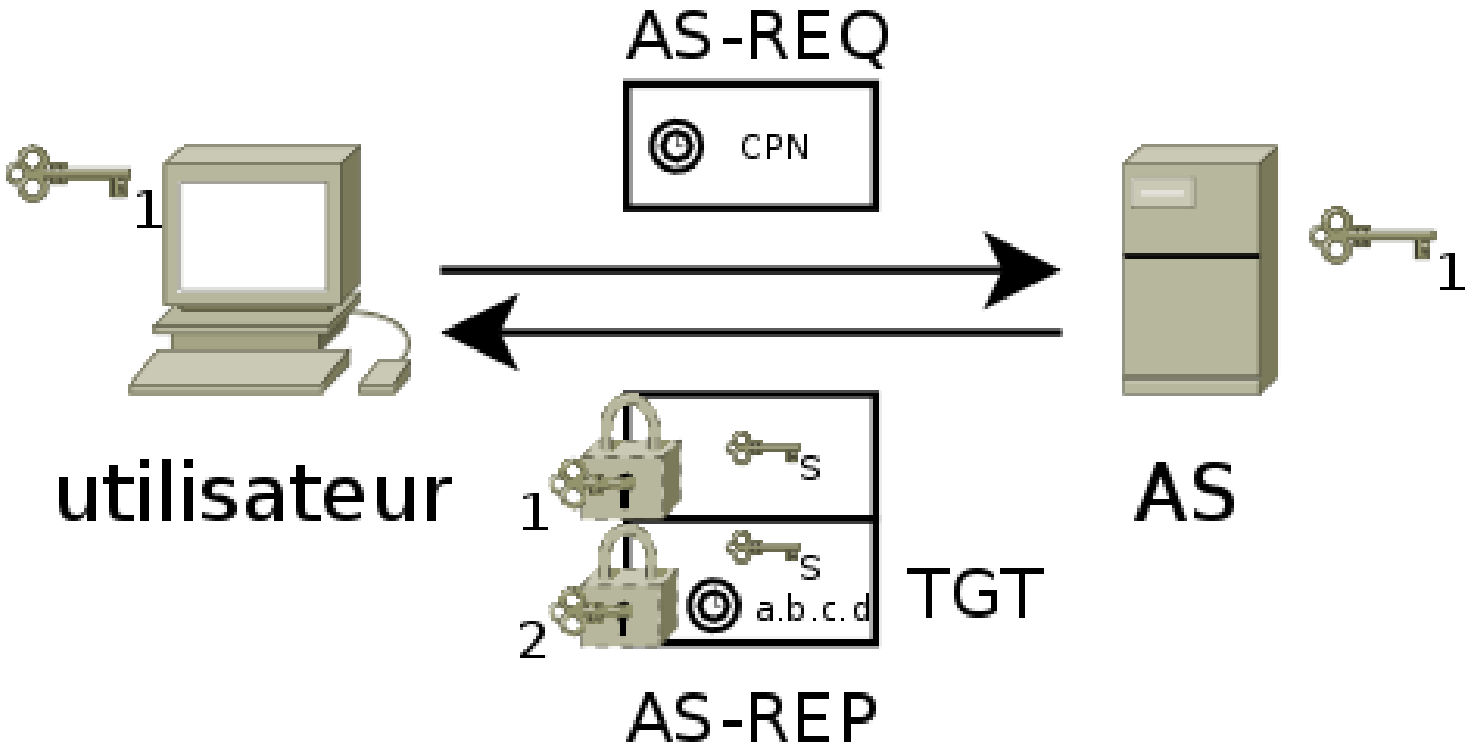
Acteurs

- client
- service
- KDC

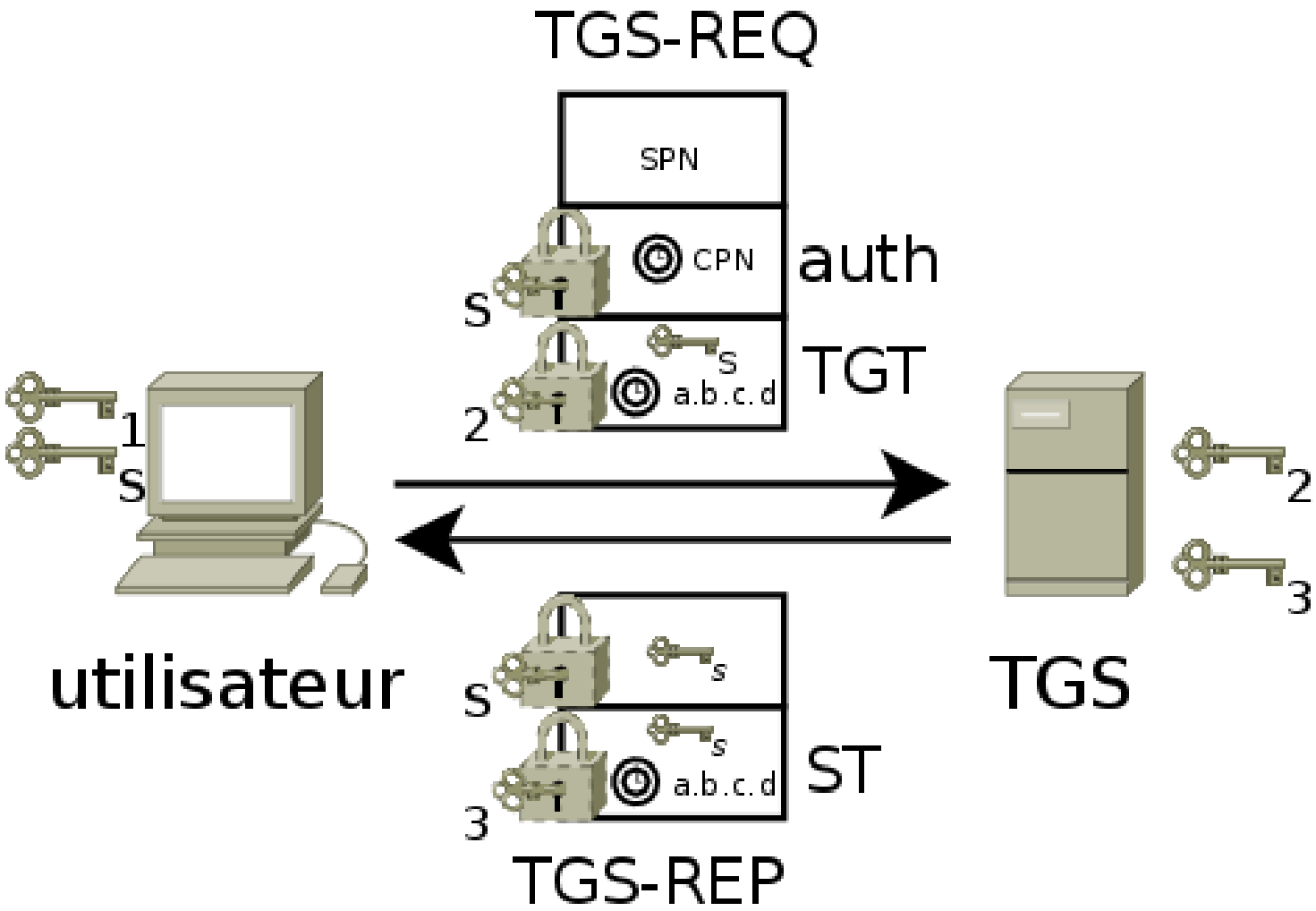
Actes

- le client s'authentifie auprès du KDC
- le client demande un ticket de service au KDC
- le client accède au service

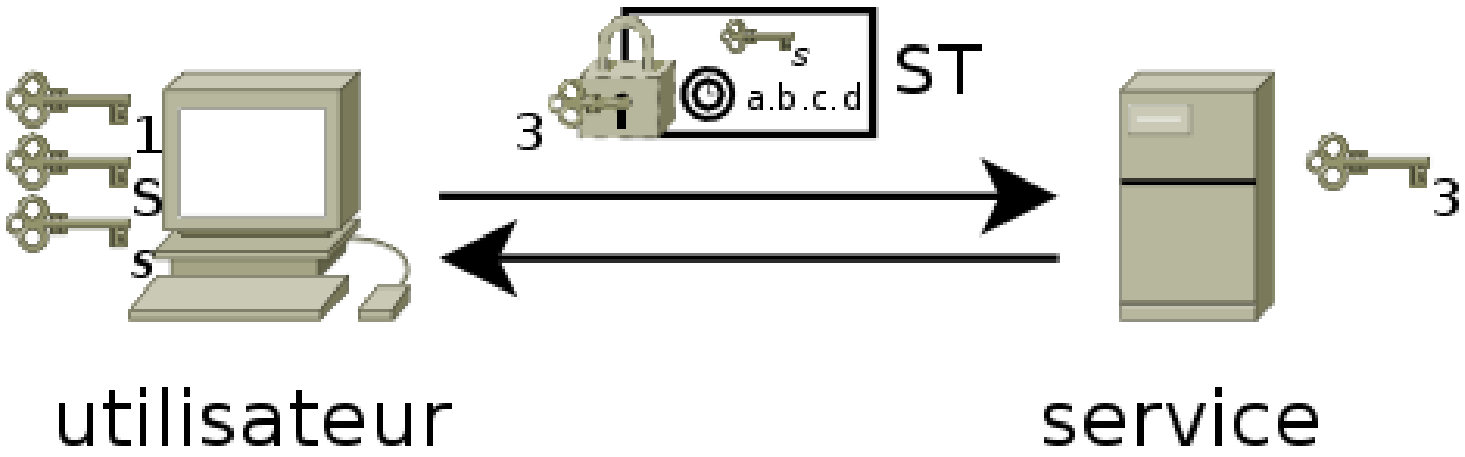
Authentification



Demande de ticket de service



Accès au service



Points remarquables

Points forts

- le mot de passe ne circule jamais
- limitation des attaques par rejeu

Points faibles

- authentification sujette à attaque hors-ligne

Points remarquables

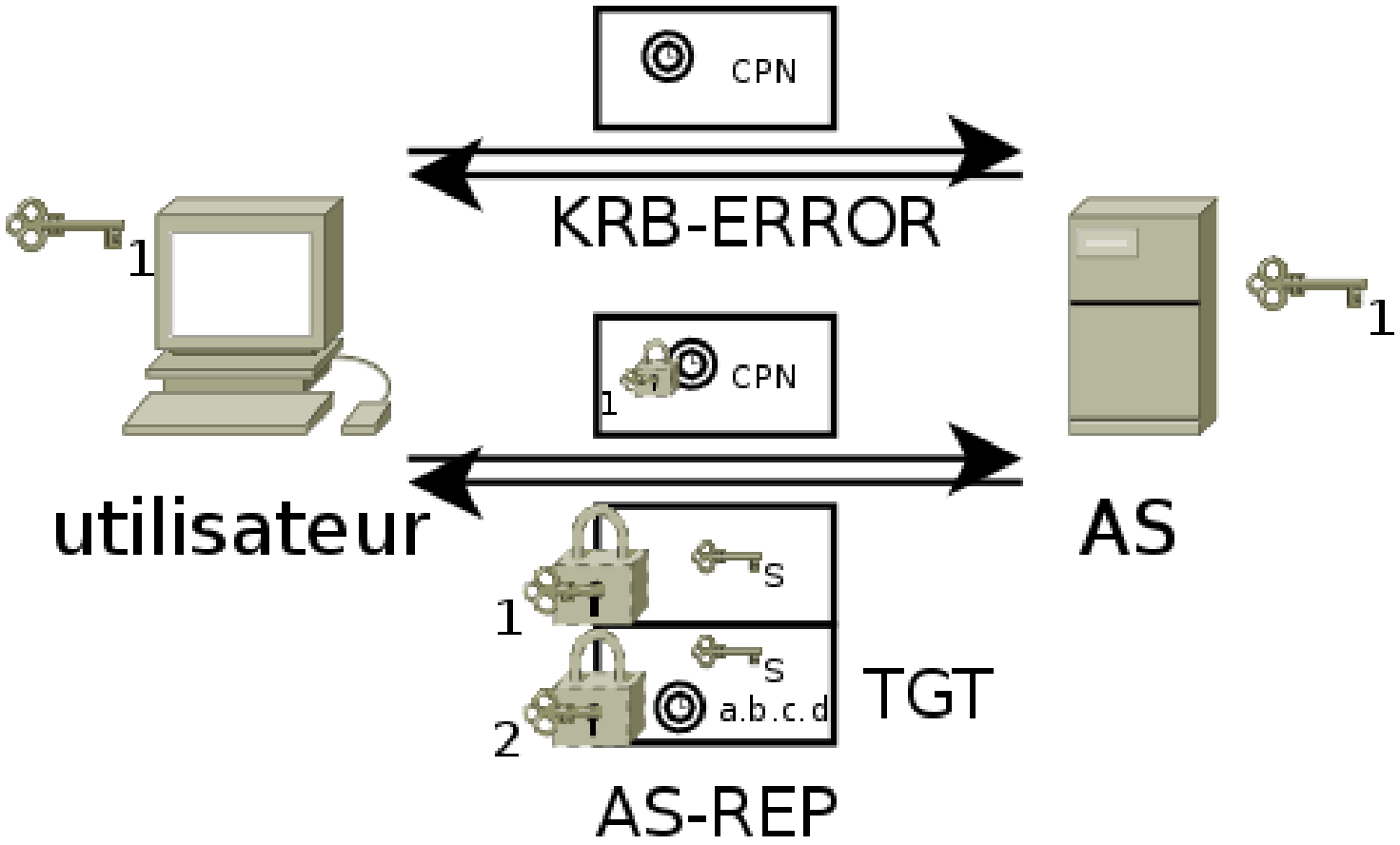
Points forts

- le mot de passe ne circule jamais
- limitation des attaques par rejeu

Points faibles

- authentification sujette à attaque hors-ligne

Pré-authentification



Plan

Ticket vs mot de passe

Authentification Kerberos

- utilisation d'un ticket
- support nécessaire au niveau du client et du protocole
- SSO et sécurité

Validation de mot de passe

- utilisation d'un mot de passe
- pas besoin de support spécifique
- ni SSO ni sécurité

Ticket vs mot de passe

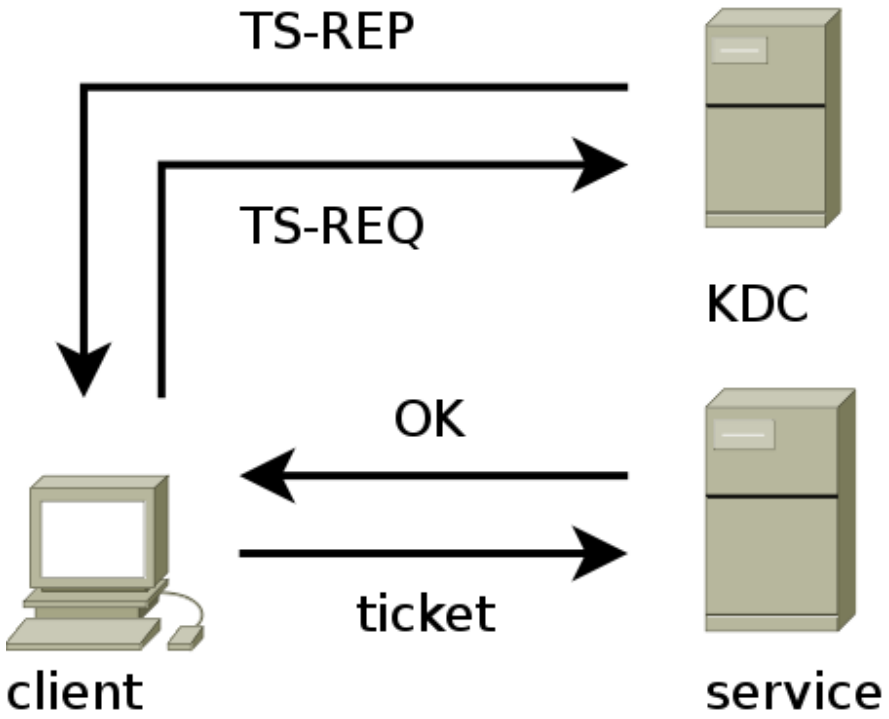
Authentification Kerberos

- utilisation d'un ticket
- support nécessaire au niveau du client et du protocole
- SSO et sécurité

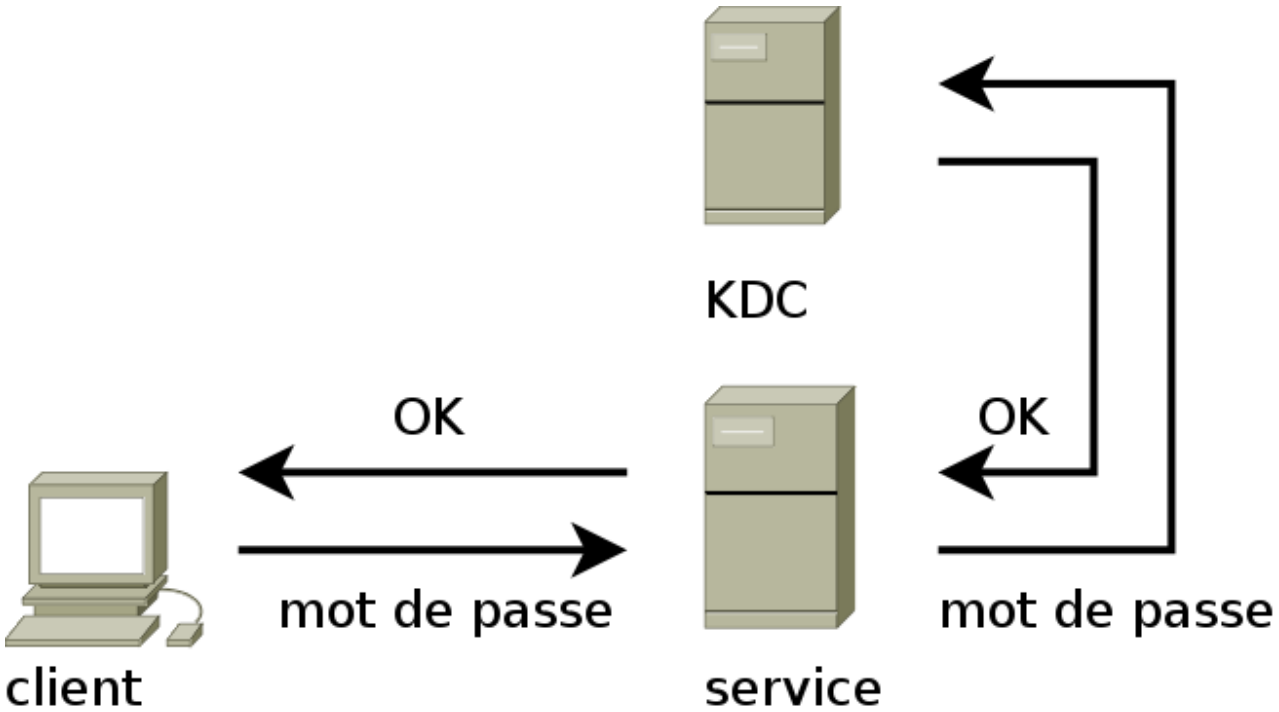
Validation de mot de passe

- utilisation d'un mot de passe
- pas besoin de support spécifique
- ni SSO ni sécurité

Authentification Kerberos



Validation de mots de passe



Plan

Site web

Negociate

Extension protocole

Support serveur

- Apache + mod_auth_kerb
- IIS

Support client

- Gecko (Firefox, ...)
- Webkit (Safari, ...)
- IE

Site web

Negociate

Extension protocole

Support serveur

- Apache + mod_auth_kerb
- IIS

Support client

- Gecko (Firefox, ...)
- Webkit (Safari, ...)
- IE

Site web

Negociate

Extension protocole

Support serveur

- Apache + mod_auth_kerb
- IIS

Support client

- Gecko (Firefox, ...)
- Webkit (Safari, ...)
- IE

Système de fichiers réseau

NFS

- support GSSAPI dans NFSv4, backporté en NFSv3
- authentification, chiffrement et contrôle d'intégrité

CIFS

- implicite au sein d'un domaine Active Directory

Système de fichiers réseau

NFS

- support GSSAPI dans NFSv4, backporté en NFSv3
- authentification, chiffrement et contrôle d'intégrité

CIFS

- implicite au sein d'un domaine Active Directory

Ouverture de session utilisateur

Session distante

- OpenSSH
- telnet

Session locale

- via pam sous Linux
- implicite au sein d'un domaine Active Directory

Ouverture de session utilisateur

Session distante

- OpenSSH
- telnet

Session locale

- via pam sous Linux
- implicite au sein d'un domaine Active Directory

Autres applications

Support GSSAPI

- ftp (proftpd, ...)
- mail (dovecot, ...
- SASL (OpenLDAP, Postfix, etc...)

Plan

Différentes implémentations

MIT

- implémentation originale
- gros effort de nettoyage en cours
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes implémentations

MIT

- implémentation originale
- gros effort de nettoyage en cours
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes implémentations

MIT

- implémentation originale
- gros effort de nettoyage en cours
- multi-plateforme

Heimdal

- conséquence des restrictions US à l'export
- base Kerberos pour Samba 4

Microsoft

- depuis windows 2000
- extension protocole : PAC

Différentes intégrations

Linux

- clients ligne de commande (kinit, klist, ...)
- clients graphique
- configuration PAM

MacOS

- implémentation MIT incluse
- interface graphique native

Windows

- application natives : support intégré à Active Directory
- certaines application tierces utilisent l'implémentation MIT

Différentes intégrations

Linux

- clients ligne de commande (kinit, klist, ...)
- clients graphique
- configuration PAM

MacOS

- implémentation MIT incluse
- interface graphique native

Windows

- application natives : support intégré à Active Directory
- certaines application tierces utilisent l'implémentation MIT

Différentes intégrations

Linux

- clients ligne de commande (kinit, klist, ...)
- clients graphique
- configuration PAM

MacOS

- implémentation MIT incluse
- interface graphique native

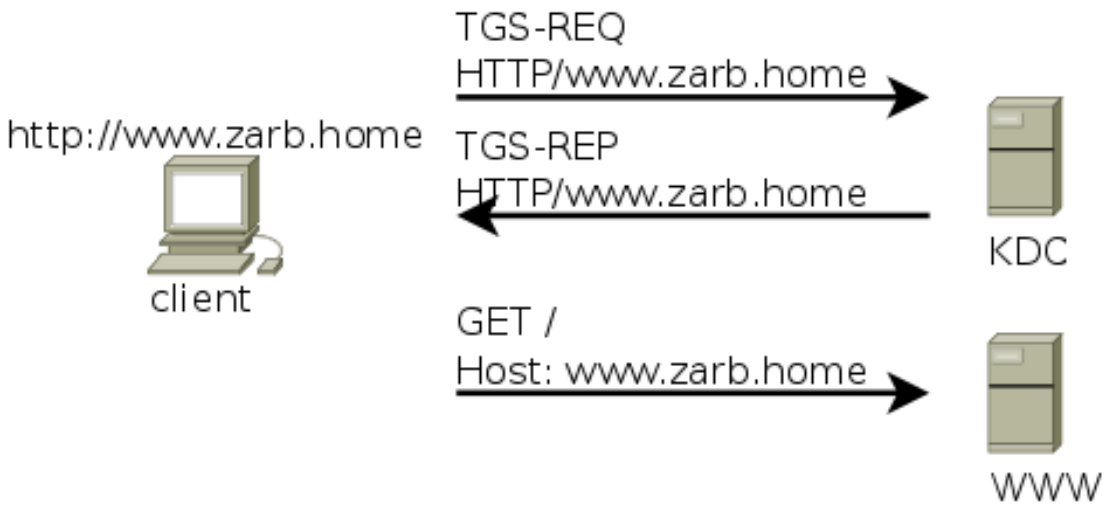
Windows

- application natives : support intégré à Active Directory
- certaines application tierces utilisent l'implémentation MIT

Différents comportements

Canonicalisation des principaux de service

Différents comportements



Principaux de service sans canonicalisation

Différents algorithmes de chiffrement

Heimdal et MIT

- AES, RC4, 3DES, ...
- DES, mais plus par défaut

Microsoft

- 2000 : DES
- 2003R2 : RC4
- 2008 : AES

Différents algorithmes de chiffrement

Heimdal et MIT

- AES, RC4, 3DES, ...
- DES, mais plus par défaut

Microsoft

- 2000 : DES
- 2003R2 : RC4
- 2008 : AES

Différents environnements

Base de comptes

- pas de comptes utilisateur
- base de comptes Posix
- base de comptes Windows

Royaumes Kerberos

- royaume unique
- royaumes multiples

Différents environnements

Base de comptes

- pas de comptes utilisateur
- base de comptes Posix
- base de comptes Windows

Royaumes Kerberos

- royaume unique
- royaumes multiples

Plan

Identifier une resource : problème

Identités multiples pour une même resource

- addresse(s) IP
- nom(s) local
- nom(s) pleinement qualifié

Objectif du protocole

Authentification réciproque

Identifier une resource : problème

Identités multiples pour une même resource

- addresse(s) IP
- nom(s) local
- nom(s) pleinement qualifié

Objectif du protocole

Authentification réciproque

Identifier une resource : solutions

Canonicalisation

Résolution du nom en principal coté client

Alias

Résolution du nom en principal coté serveur

Multiplication des principaux

Multiple principaux pour un même service

Identifier une resource : solutions

Canonicalisation

Résolution du nom en principal coté client

Alias

Résolution du nom en principal coté serveur

Multiplication des principaux

Multiple principaux pour un même service

Identifier une resource : solutions

Canonicalisation

Résolution du nom en principal coté client

Alias

Résolution du nom en principal coté serveur

Multiplication des principaux

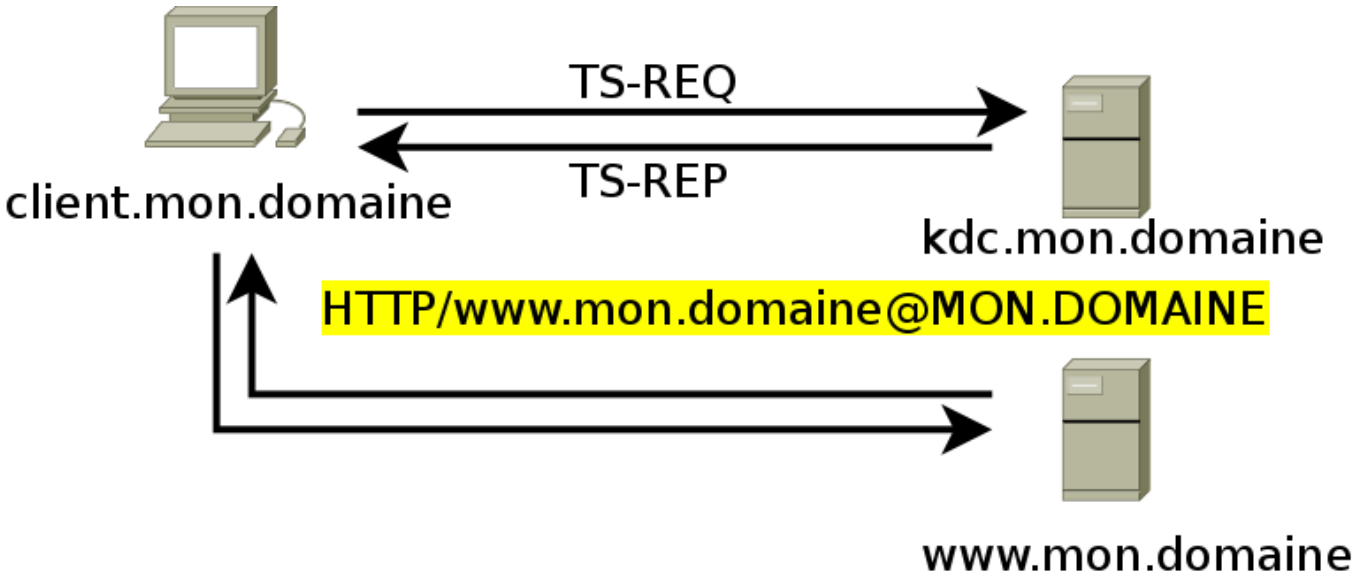
Multiple principaux pour un même service

Domaine Kerberos multiples : problème

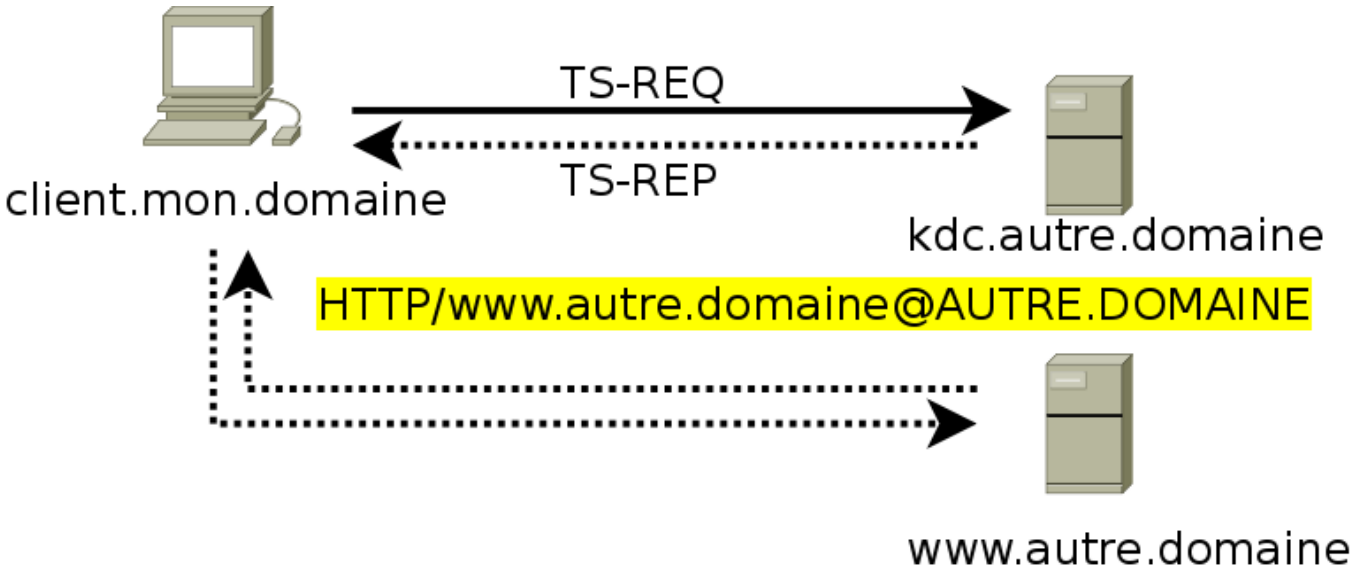
Problème

- accéder à une ressource dans un autre domaine
- obtenir un ticket pour cette ressource de son KDC
- impossible de s'authentifier auprès de ce KDC

Service du domaine



Service d'un autre domaine, sans confiance

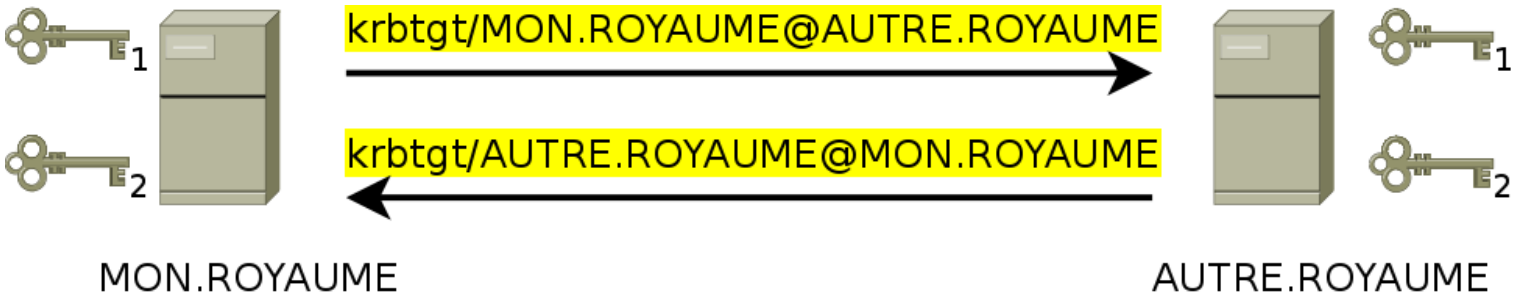


Domaine Kerberos multiples : solution

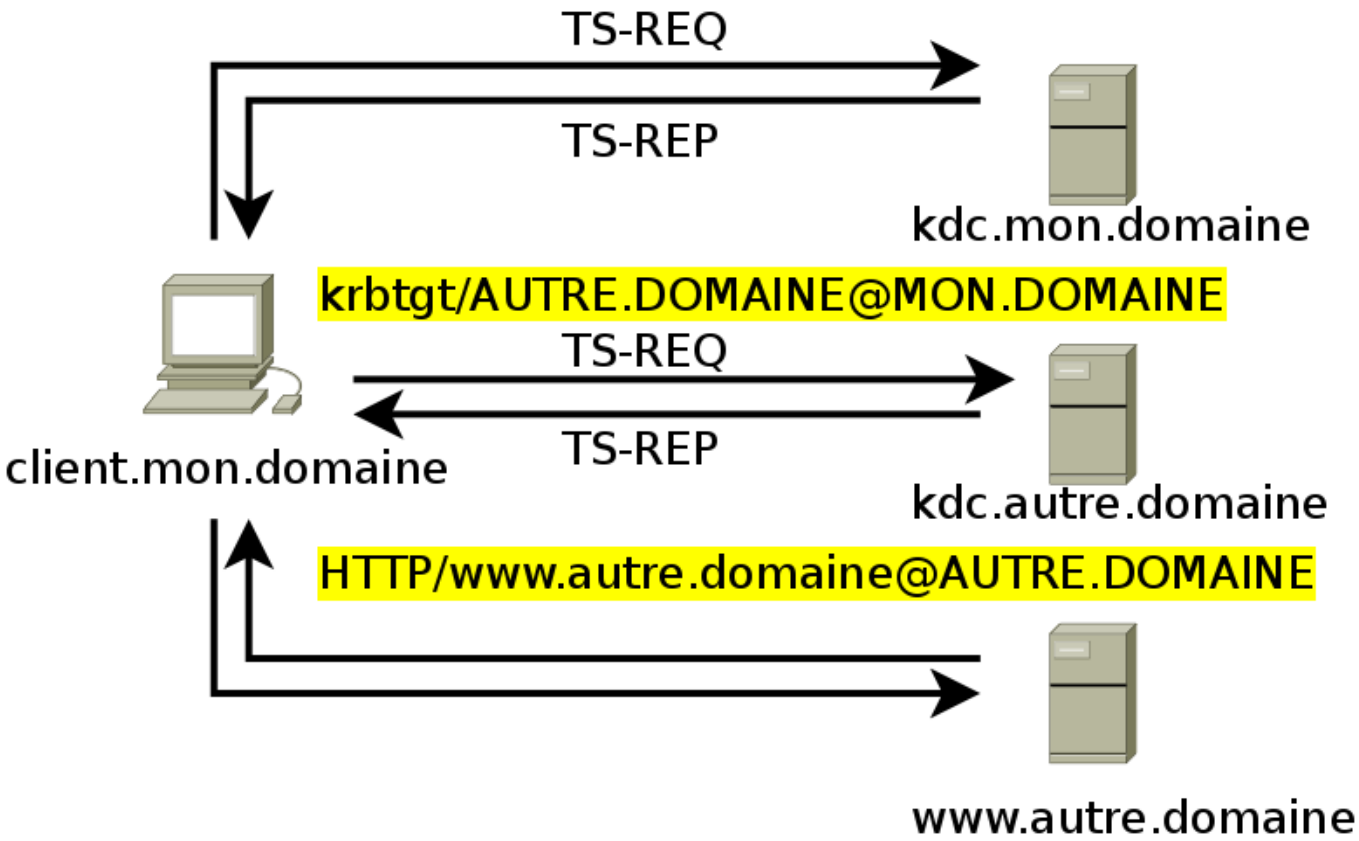
Solution

Relation de confiance entre royaumes Kerberos

Relation de confiance



Service d'un autre domaine, avec confiance



Confiance entre implémentations différentes

Heimdal et MIT

Aucun souci

Microsoft et non-Microsoft

- configuration base de registre sur chaque client
- configuration relation de confiance :
  - type de la clé
  - protocole transport (TCP conseillé)

Confiance entre implémentations différentes

Heimdal et MIT

Aucun souci

Microsoft et non-Microsoft

- configuration base de registre sur chaque client
- configuration relation de confiance :
  - type de la clé
  - protocole transport (TCP conseillé)

Duplication des données : problème

Plusieurs listes d'utilisateur

- compte(s) utilisateur
- principaux Kerberos

Plusieurs mots de passe

- mot de passe lié au compte
- mot de passe Kerberos

Duplication des données : problème

Plusieurs listes d'utilisateur

- compte(s) utilisateur
- principaux Kerberos

Plusieurs mots de passe

- mot de passe lié au compte
- mot de passe Kerberos

Duplication des données : solutions

Synchronisation

Les données d'un système sont répliquées vers un autre

- protocole LDAP pour les annuaires
- protocole kadmin pour Kerberos

Intégration

Deux système utilisent une même source de données

- stockage LDAP pour la base Kerberos

Duplication des données : solutions

Synchronisation

Les données d'un système sont répliquées vers un autre

- protocole LDAP pour les annuaires
- protocole kadmin pour Kerberos

Intégration

Deux système utilisent une même source de données

- stockage LDAP pour la base Kerberos

Duplication des données : solutions (suite)

Délégation

Une fonctionalité d'un des systèmes est réalisée par un autre

- authentification pass-through dans OpenLDAP
- greffon krb5smb pour OpenLDAP
- altSecurityIdentities dans Active Directory

Remplacement

Un système remplace un autre

- Active Directory + winbind
- Active Directory + SFU
- LDAP + Kerberos + Samba 4 ?

Duplication des données : solutions (suite)

Délégation

Une fonctionalité d'un des systèmes est réalisée par un autre

- authentification pass-through dans OpenLDAP
- greffon krb5smb pour OpenLDAP
- altSecurityIdentities dans Active Directory

Remplacement

Un système remplace un autre

- Active Directory + winbind
- Active Directory + SFU
- LDAP + Kerberos + Samba 4 ?

Plan

Kerberos, c'est bien(tm)

Avantages multiples

- authentification forte
- standardisation
- SSO de bout en bout

Mais pas trivial

Complexité certaine

- objectif ambitieux
- hétérogénéité environnement

Non insurmontable

- peu d'impact sur l'utilisateur final
- évolution de la spécification

Mais pas trivial

Complexité certaine

- objectif ambitieux
- hétérogénéité environnement

Non insurmontable

- peu d'impact sur l'utilisateur final
- évolution de la spécification

Et surtout pas suffisant

Solutions plausibles

- Active Directory + émulation POSIX
- Active Directory + annuaire LDAP + base Kerberos

Contexte utilisateurs

- systèmes d'exploitation
- modes d'administration

Et surtout pas suffisant

Solutions plausibles

- Active Directory + émulation POSIX
- Active Directory + annuaire LDAP + base Kerberos

Contexte utilisateurs

- systèmes d'exploitation
- modes d'administration